



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/787,575	04/08/2002	John W. Halpern	HALJW/102/PC/US	5239
2543	7590	12/13/2005	EXAMINER	
ALIX YALE & RISTAS LLP 750 MAIN STREET SUITE 1400 HARTFORD, CT 06103			BROWN, CHRISTOPHER J	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 12/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/787,575	Applicant(s) HALPERN, JOHN W.	
	Examiner Christopher J. Brown	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 April 2002.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☒ Claim(s) 2,4,5,6,8,9,10,17 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 08 April 2002 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☒ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Specification

The disclosure is objected to because of the following informalities: the specification is not uniform, and it does not appear to be in the proper USPTO format.

Appropriate correction is required.

Drawings

New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because some of the drawings appear to be of an informal nature and some items do not have labels. Applicant is advised to employ the services of a competent patent draftsman outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Claim Objections

1. Claims 2, 4, 5, 6, 8, 9, 10, and 17 objected to because of the following informalities:

Claims 2, 4, 5, 6, 8, 9, 10, and 17 include numerous abbreviations in parenthesis. The abbreviations are unnecessary and do not help further the limitations of the claims.

Appropriate correction is required.

As per claim 8 line 1, the examiner believes the word "renewals" should be "renewal".

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim 5 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. As per claim 5, the applicant is claiming an email system with a switchboard for a direct connection. It is

obvious to one of ordinary skill in the art that email systems do not connect directly, and thus do not need switchboards.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 1, line 31 states "key numbers" it is unclear whether "key numbers" refers to the keys previously stated in claim 1, or are a different entity.

As per claim 1, line 32 states "shift register-like memory structure". It is unclear whether the applicant is claiming a shift register. A shift register-like memory structure is indefinite as to make the claim unclear to the examiner.

As per claim 1, the applicant states "random keys", "said keys" and "a new key", and "other keys". It is unclear in the claim that when the applicant states "said keys" to which key he is referring, or if the keys with different names are actually the same key.

For example it appears the "random keys" on line 9 and "new key" on line 26 are actually the same key. Appropriate correction is required.

As per claim 1 lines 19, and 20, the use of the word "associated" is indefinite. It is unclear in what way or how the key is related to an address code, or how the address code is related to data indicative of the age of the key.

Art Unit: 2134

As per claim 2, it is unclear if “key numbers” are referring to the keys, or the key numbers of claim 1, or if the keys and key numbers are the same thing.

As per claim 3 the term “assist” in line 24 is indefinite. It is unclear how the address “assists” the server station. Appropriate correction is required.

As per claim 6, the term “quasi data inputs” is indefinite. It is not clear what the applicant means by “quasi data inputs”. Specifically “quasi” is confusing and indefinite.

As per claim 8, the applicant refers to multiple instances of registers without differentiating between registers. Appropriate correction is required.

As per claim 8, the claim lacks antecedent basis because of the term “said initial meaningless random information” appropriate correction is required.

As per claim 10, the claim lacks antecedent basis for the term “operative key number”.

Claim 12 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: Claim 12 is missing a step wherein the email station sends a decrypted check number to the server.

Claim 12 is indefinite because it does not state to who it will “execute the call repeating the verification steps....”.

Claim 17 lacks antecedent basis for ID and CC on page17 line 19.

Claims 14, 15, 16, 18, and 19 are indefinite because it states “continually influenced and modified”. This statement gives no indication of how the circuit is modified, it is unclear how the bits are influencing the encryption circuit, therefore the claim is indefinite.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 2 and 9, are rejected under 35 U.S.C. 103(a) as being unpatentable over Kadansky US 6,295,361 in view of Trieiger US 6,226,750 in view of Linehan US 5,495,533.

As per claims 1, and 9 Kadansky teaches a key renewal system for confidential communications between at least two stations linked to a communications system, (Col 7 line 55- Col 8 line 15).

Kadansky teaches that prior to confidential communication, a renewal of keys used by at least two stations is performed so that the stations can encrypt data to be transmitted using said keys, (Col 7 line 55-Col 8 line 15). Kadansky does not teach random key generation. Kadansky does not teach storing keys in a lookup table.

Trieiger teaches random key generation for distribution from a server to a client, (Col 11 lines 30-35). Trieiger teaches storing keys in a lookup table with relative ages, (Col 11 lines 33-44). Trieiger teaches that keys may be moved from younger to older positions and invalidated, (Col 11 lines 36-44). Trieiger does not teach an address associated with keys in a lookup table.

Art Unit: 2134

It would have been obvious to one of ordinary skill in the art to use the random key generation of Trieger with the key distribution system of Kadansky because randomly generated keys are more difficult to crack.

Linehan teaches a method where a client sends a key index number to a server in order for the server to access the clients key, (Col 9 lines 42-47). It would have been obvious to use the key index number of Linehan with the previous Kadansky-Trieger combination because it allows quicker access to said key.

As per claim 2, Kadansky teaches encryption and a key replacement routine, (Col 7 line 40-Col 8 line 15).

Claims 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kadansky US 6,295,361 in view of Trieger US 6,226,750 in view of Linehan US 5,495,533 in view of Kato US 6,343,281

As per claim 3, the previous Kadansky-Trieger-Linehan combination teaches a system wherein an address is sent to find a key, and distributing the key. Kadansky-Trieger-Linehan does not teach a key encrypting itself and decrypting said key to compare for authenticity.

Kato teaches encrypting a key with itself, (Col 6 lines 16-20). Kato teaches decrypting said key and comparing it with itself, (Col 8 line 60 Col 9 line 4).

It would have been obvious to one of ordinary skill in the art to use the key encryption method of Kato with the system of of Kadansky-Trieger-Linehan because encryption increases the security of the system.

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kadansky US 6,295,361 in view of Triegeer US 6,226,750 in view of Linehan US 5,495,533 in view of Kato US 6,343,281 in view of Naor US 6,275,573

As per claim 4, the previous Kadansky-Triegeer-Linehan-Kato combination does not teach encrypting a key from the server with a key of the client.

Naor teaches a key exchange method where the key of the server is encrypted with the previously exchanged public key of the client, (Col 5 lines 20-35).

It would have been obvious to one of ordinary skill in the art to use the key exchange method of Naor with the previous combination of Kadansky-Triegeer-Linehan-Kato, because it increases the security of key exchange.

Claims 6, 11, 13, 14, 15, 18 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kadansky US 6,295,361 in view of Triegeer US 6,226,750 in view of Linehan US 5,495,533 in view of Kato US 6,343,281 in view of Naor US 6,275,573 in view of Beutelspacher US 4,974,193.

As per claims 6, 11, 13, 14, 15, 18, and 19 the previous Kadansky-Triegeer-Linehan-Kato-Naor combination does not teach a random start time. Beutelspacher teaches a random start time, (Col 2 lines 50-60).

It would have been obvious to one of ordinary skill in the art to modify the system with a random start time because it enhances the complexity of the encryption algorithm.

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kadansky US 6,295,361 in view of Triegeer US 6,226,750 in view of Linehan US 5,495,533 in view of Kato US 6,343,281 in view of Naor US 6,275,573 in view of Sullivan US 5,351,296

The previous Kadansky-Triegeer-Linehan-Kato-Naor combination does not teach a word-bit between 8 and 16 bits. Sullivan teaches a word-bit that is 12 bits, (Col 7 lines 53-55). It would have been obvious to one of ordinary skill in the art to use a word between 8 and 16 bits because it enables a greater variety of memory usage.

Claims 10, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kadansky US 6,295,361 in view of Triegeer US 6,226,750 in view of Linehan US 5,495,533 in view of Jennings III US 6,134,631

As per claims 10, and 16 the previous Kadansky-Triegeer-Linehan combination does not teach a password.

Jennings III teaches a password to protect access to keys, (Col 6 lines 1-10).

It would be obvious to one of ordinary skill in the art to use a password to protect the key thus enhancing security.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kadansky US 6,295,361 in view of Triegeer US 6,226,750 in view of Linehan US 5,495,533 in view of Naor US 6,275,573, in view of Matais 6,681,017.

As per claims 12 Kadansky teaches a key renewal system for confidential communications between at least two stations linked to a communications system, (Col 7 line 55- Col 8 line 15).

Kadansky teaches that prior to confidential communication, a renewal of keys used by at least two stations is performed so that the stations can encrypt data to be transmitted using said keys, (Col 7 line 55-Col 8 line 15). Kadansky does not teach random key generation. Kadansky does not teach storing keys in a lookup table.

Trieger teaches random key generation for distribution from a server to a client, (Col 11 lines 30-35). Trieger teaches storing keys in a lookup table with relative ages, (Col 11 lines 33-44). Trieger teaches that keys may be moved from younger to older positions and invalidated, (Col 11 lines 36-44). Trieger does not teach an address associated with keys in a lookup table.

It would have been obvious to one of ordinary skill in the art to use the random key generation of Trieger with the key distribution system of Kadansky because randomly generated keys are more difficult to crack.

Linehan teaches a method where a client sends a key index number to a server in order for the server to access the clients key, (Col 9 lines 42-47). It would have been obvious to use the key index number of Linehan with the previous Kadansky-Trieger combination because it allows quicker access to said key. The Kadansky-Trieger-Linehan combination does not teach a random check included in communication.

Naor teaches a key exchange method where the key of the server is encrypted with the previously exchanged public key of the client, (Col 5 lines 20-35).

Art Unit: 2134

It would have been obvious to one of ordinary skill in the art to use the key exchange method of Naor with the previous combination because it increases the security of key exchange.

Matais teaches including a random nonce in communications, (Col 2 lines 40-45). It would have been obvious to one of ordinary skill in the art to include the random nonce because it helps verify the communication.

Claim 17 rejected under 35 U.S.C. 103(a) as being unpatentable over Kadansky US 6,295,361 in view of Triege US 6,226,750 in view of Linehan US 5,495,533 in view of Kato US 6,343,281 in view of Naor US 6,275,573 in view of Beutelspacher US 4,974,193 in view of Matias US 6,681,017.

The previous Kadansky-Triege-Linehan-Kato-Naor-Beutelspacher combination does not teach a write once memory with identification information.

Matias teaches a write once memory with identification information, (Col 1 lines 10-20).

It would have been obvious to one of ordinary skill in the art to include the identification information on memory because it allows one to easily acquire information about the device.

Conclusion


4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J. Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

Art Unit: 2134

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher J. Brown

12/7/05



GREGORY MORSE
SUPERVISOR PATENT EXAMINER
ELECTRONIC BUSINESS CENTER 2100